UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,192	12/02/2003	Simon Robert Walmsley	PEA17US	4559

24011 7590 02/03/2010
SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
02/03/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

pair@silverbrookresearch.com
patentdept@silverbrookresearch.com
uscorro@silverbrookresearch.com

Office Action Summary	**Application No.** 10/727,192	**Applicant(s)** WALMSLEY ET AL.	
	Examiner NADIA KHOSHNOODI	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/7/2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claim 4 has been cancelled. Applicant's arguments/amendments with respect to pending claims 1-3 & 5-32 filed 10/7/2009 have been fully considered but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants contend that in Husemann the secret key is known to two other entities "and is therefor not allocated to only a first entity as required by the claimed invention and neither Wertheimer nor Schneier provide any disclosure which makes up for this deficiency in Husemann." Examiner respectfully disagrees. First, Examiner would like to clarify that it is presumed that Applicants are referring to the amended limitation in their arguments, since the terminology claimed ("primary entity") was not exactly the terminology used in the arguments ("first entity"). Second, Examiner would like to note that Husemann was not cited to teach the limitation "allocating a first secret key to the primary entity," which was presented prior to the amendments filed 10/7/2009. Wertheimer col. 6, lines 53-57 were cited to meet this limitation. Currently, Applicants have argued that Husemann fails to teach the amended limitation, which actually reads "allocating, in a computer system, a first secret key to only the primary entity." In reference to this argument, Examiner would like to point out that Husemann was/is not relied upon to meet this claimed limitation. Wertheimer teaches that a computer system generates a public key and a secret key, where this key is allocated to the user for use in encrypting messages (col. 6, lines 51-53). Wertheimer also teaches the use of key escrow agents with which the key

may be communicated (col. 6, lines 53-57), however this does not teach away from the limitation “allocating, in the computer system, a first secret key to only the primary entity." Applicants may have intended to specifically claim that the secret key is not shared with any other entities, however that is not the scope of what is actually being claimed. The term "allocating" does not suggest that the first secret key may not be communicated over a trusted network with escrow agents for backup purposes, it merely means that the first secret key is only assigned to the primary entity. Absent any contrary definition for the term “allocating” in the Applicants' Disclosure, Examiner interprets allocating a first secret key to only the primary entity as assigning a secret key to one entity, i.e. the primary entity. Thus, with this interpretation (according to MPEP 2111) and since Wertheimer teaches that the secret key is generated by a computer and assigned to only one user, the fact that the secret key is shared with escrow agents in Wertheimer for backup is irrelevant.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner’s conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-3, 5-16, 18-20, 22-24, 26-28, and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wertheimer et al., US Patent No. 5,920,630 and further in view of Husemann et al., US Patent No. 6,192,349.

As per claim 1:

Wertheimer et al. substantially teach a method including the steps of: allocating, in the computer system, a first secret key to only the primary entity (col. 6, lines 53-57); for each of the one or more secondary entities, determining, in the computer system, a second secret key by applying a one way function to that secondary entity's identifier and the first secret key (col. 6, line 65 – col. 7, line 11), such that the second secret key is a variant of the first secret key only ascertainable with knowledge of the first secret key from the primary entity (col. 6, line 65 – col. 7, line 11); allocating, in the computer system, the second secret key to the or each secondary entity (col. 7, lines 12-25).

Not explicitly disclosed is applying the one way function to only the secondary entity's identifier and the first secret key. However, Husemann et al. teach that, in an environment that makes use of smart cards owned by one or more secondary entities, a secret key for each card can be generated by performing a hash over a master key and the card's identifier (col. 2, lines 45-51). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wertheimer et al. to create the secret key from only a primary key and the secondary entity's identifier. This modification would have been obvious (in light of *KSR*) because a person having ordinary skill in the art, at the time the invention was made, could have generated a key in the manner claimed since Husemann et al. suggest that one

of ordinary skill in the art could have used only a primary entity's key and a secondary entity's identifier to generate a secret key in col. 2, lines 45-51.

As per claim 2:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach wherein the identifiers allocated to the secondary entities are generated stochastically, pseudo-randomly or arbitrarily (col. 8, lines 53-67).

As per claim 3:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 2. Furthermore, Wertheimer et al. teach wherein the one-way function is a hash function (col. 9, lines 8-15).

As per claim 5:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 3. Furthermore, Wertheimer et al. teach wherein the one-way function is a Secure Hash Algorithm function (col. 9, lines 8-15).

As per claim 6:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach wherein each of the entities is implemented in an integrated circuit (col. 6, lines 25-50).

As per claim 7:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach wherein each of the entities is implemented in an integrated circuit separate from the integrated circuits in which the other entities are

implemented (col. 6, lines 25-50).

As per claim 8:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach wherein one or more of the secondary entities are implemented in a corresponding plurality of integrated circuits (col. 6, lines 25-50).

As per claim 9:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach wherein the primary entity is implemented in an integrated circuit (col. 6, lines 25-50).

As per claim 10:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach wherein both the primary and secondary entities are implemented in integrated circuits (col. 6, lines 25-50).

As per claim 11:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach in which the first entity wishes to communicate with one of the second entities, the method including the steps, in the first entity, of: receiving data from the second entity (col. 6, line 53 – col. 7, line 11); using the data and the first secret key to generate the second secret key associated with the second entity (col. 6, line 53 – col. 7, line 11).

As per claim 12:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 11. Furthermore, Wertheimer et al. teach wherein the data contains an identifier for the second entity (col. 6, line 65 – col. 7, line 11).

As per claim 13:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 11. Furthermore, Wertheimer et al. teach in which the first entity wishes to send an authenticated message to the second entity, the method including the steps, in the first entity, of: using the generated second secret key to sign a message, thereby generating a digital signature; outputting the message and the digital signature for use by the second entity, which can validate the message by using the digital signature and its own copy of the second secret key (col. 10, lines 19-37).

As per claim 14:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 13. Wertheimer further teach the method in which the generated signature includes its own copy of the second secret key and in which the generated signature includes a nonce from the first entity, and the output from the first entity includes the nonce, thereby enabling the second entity to validate the message using the digital signature, the nonce (col. 12, lines 43-51).

As per claim 15:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 11. Furthermore, Wertheimer et al. teach wherein the data contains a first nonce (col. 12, lines 43-51).

As per claim 16:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 15. Furthermore, Wertheimer et al. teach the method in which the first entity wishes to send an authenticated message to the second entity, the method including the steps, in the first entity, of: using the generated second secret key and the nonce to sign a message, thereby generating a digital signature; outputting the message and the digital signature for use by the second entity, which can validate the message by using the digital signature and its own copy of the second secret key (col. 12, lines 43-60).

As per claim 18:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 11. Furthermore, Wertheimer et al. teach the method in which the first entity wishes to send an encrypted message to the second entity, the method including the steps, in the first entity, of: using the generated second secret key to encrypt a message, thereby generating an encrypted message; outputting the encrypted message for use by the second entity, which can decrypt the message by using its own copy of the second secret key (col. 9, lines 49-61).

As per claim 19:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 18. Furthermore, Wertheimer et al. teach the method in which the encrypted message includes a nonce from the first entity, and the output from the first entity includes the nonce, thereby enabling the second entity to decrypt the message using the nonce, and its own copy of the second secret key (col. 12, lines 43-51).

As per claim 20:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 15. Furthermore, Wertheimer et al. teach the method in which the first entity wishes to send an encrypted message that incorporates the first nonce to the second entity, the method including the steps, in the first entity, of: using the generated second secret key to encrypt a message and the first nonce, thereby generating an encrypted message; outputting the encrypted message for use by the second entity, which can decrypt the encrypted message by using its own copy of the second secret key (col. 10, lines 19-37).

As per claim 22:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: using the second secret key to sign a message, thereby to generate a digital signature; and outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby authenticate the message via the digital signature (col. 10, lines 19-37).

As per claim 23:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: using the second secret key and a nonce to sign a message, thereby to generate a digital signature; and outputting the message, nonce, digital signature and the second entity's

identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby authenticate the message via the nonce and digital signature (col. 12, lines 43-60).

As per claim 24:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: receiving a first nonce from the first entity; using the second secret key and the first nonce to sign a message, thereby to generate a digital signature; and outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby authenticate the message via the first nonce and digital signature (col. 11, lines 2-40 and col. 12, lines 43-51).

As per claim 26:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: using the second secret key to encrypt the message, thereby to generate an encrypted message; and outputting the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby decrypt the encrypted message

(col. 9, lines 20-61).

As per claim 27:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: using the second secret key to encrypt the message and a nonce, thereby to generate an encrypted message; and outputting the nonce, encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby decrypt the encrypted message (col. 10, lines 40-58).

As per claim 28:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: receiving a nonce from the first entity; using the second secret key to encrypt the message and the nonce, thereby to generate an encrypted message; and outputting the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby decrypt the encrypted message (col. 10, lines 51-64).

As per claim 30:

Wertheimer et al. and Husemann et al. substantially teach the method according to any one of claims 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 27, 28 or 29 (i.e. claim 14). Furthermore,

Wertheimer et al. teach wherein at least one of the nonces is a pseudo-random number (col. 10, lines 59-64).

As per claim 31:

Wertheimer et al. and Husemann et al. substantially teach the method according to any one of claims 11 to 21 (i.e. claim 11). Furthermore, Wertheimer et al. teach wherein the communication is an authenticated read of a field of the first entity (col. 7, lines 1-31).

As per claim 32:

Wertheimer et al. and Husemann et al. substantially teach the method according to any one of claims 22 to 29 (i.e. claim 22). Furthermore, Wertheimer et al. teach wherein the communication is an authenticated read of a field of the second entity (col. 7, lines 1-31).

IV. Claims 17, 21, 25, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wertheimer et al., US Patent No. 5,920,630 and Husemann et al., US Patent No. 6,192,349, as applied to claims 1, 3, 16, and 20 above, and further in view of Bruce Schneier, *Applied Cryptography*.

As per claim 17:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 16. Not explicitly disclosed is the method in which the generated signature includes a second nonce from the first entity, and the output from the first entity includes the second nonce, thereby enabling the second entity to validate the message using the digital signature, the first and second nonces, and its own copy of the second secret key. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made

to modify the method disclosed in Wertheimer et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."

As per claim 21:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 20. Not explicitly disclosed is the method in which the encrypted message includes a second nonce from the first entity, and the output from the first entity includes the second nonce. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wertheimer et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."

As per claim 25:

Wertheimer et al. and Husemann et al. substantially teach the method according to claim 1. Furthermore, Wertheimer et al. teach the method in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of: receiving a first nonce from the first entity; using the second secret key and the first

nonce, thereby to generate a digital signature; and outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret key to generate the second secret key associated with the second entity, and thereby authenticate the message via the first nonce, and digital signature (col. 10, lines 51-64).

Not explicitly disclosed is using a second nonce in generating a signature for the message, outputting the second nonce, and authenticating the second nonce. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wertheimer et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section “Signing Documents and Timestamps.”

As per claim 29:

Wertheimer et al. and Husemann et al. substantially teach method according to claim 1. Furthermore, Wertheimer et in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of: receiving a first nonce from the first entity; using the second secret key to encrypt the message and the first nonce, thereby to generate an encrypted message; and outputting, the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier

and the first secret key to generate the second secret key associated with the second entity, and thereby decrypt the encrypted message (col. 10, lines 51-64).

Not explicitly disclosed is encrypting a second nonce and outputting a second nonce. However, Schneier teaches that timestamps may be used in combination with digital signatures in order to prevent against replay attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wertheimer et al. to use timestamps with digital signature technology in order to prevent from various attacks. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Schneier suggests that timestamps prevent replay attacks on page 38, third paragraph under section "Signing Documents and Timestamps."

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
1/29/2010

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437